行政院及所屬各機關因公出國人員報告書

（出國類別：其他）

參加「芝加哥聯邦準備銀行金融機構監理專業課程：E-Banking/Mobile Banking」摘要與心得報告

服務機關：金融監督管理委員會檢查局

姓名職稱：李偉旭　稽查

派赴國家：美國

出國期間：2016 年　6 月 18 日 至 27 日

報告日期：2016 年　9 月 1 日

參加「芝加哥聯邦準備銀行金融機構監理專業課程：E-Banking/Mobile Banking」

摘要

金融服務業相較於其他產業高度倚賴電子化（e 化）資訊系統，而電子化不僅使金融機構經營效率大幅提升，**而網路科技發展與金融創新應用的趨勢，更促進金融科技發展並改變原有經營傳統實體分行通路思維，e 化通路程度成為未來金融機構擴大交易與服務層面的競爭力關鍵，**電子銀行/行動銀行（E-Banking/Mobile Banking）逐漸對傳統金融機構所提供之實體分行服務造成衝擊與壓力，因此為增進世界各國金融監理檢查人員對電子銀行/行動銀行監理重點之瞭解及交流檢查經驗，**芝加哥聯邦準備銀行於 105 年 6 月 20 日至 24 日在美國芝加哥主辦「E-Banking/Mobile Banking」研討會，邀請芝加哥美國聯邦準備銀行 5 位資深檢查人員擔任講師，與學員一起研討電子銀行/行動銀行討論技術基礎，並從技術發展趨勢中掌握辨識、評估、管理和監控科技風險之能力。**

本次「E-Banking/Mobile Banking」研討會特色是**以電子銀行/行動銀行之技術和風險為主軸，主題包括電子銀行/行動金融服務技術概論、常見的網路安全威脅和漏洞、Web 伺服器測試、網路身分認證及 Web 應用程式測試，實機測試(Lab 課程)則包括網站的安全評估、漏洞測試和 SQL 隱碼攻擊（SQL Injection），以及如何評估及控制管理上開資訊科技風險。**

本次共有 24 位金融監理人員參與研討會，其中大多數為美國監理人

員，有 17 位是美國本土監理機關派來參訓人員，如：FDIC、OCC、FRB District(FRB Boston、Kansas、Chicago 及 San Francisco)等，另外 7 位參訓人員是來自全球其他國家監理機構，分別是我國、印度、香港、巴西、南韓、亞美尼亞及俄羅斯。上課主軸議題為電子銀行/行動銀行趨勢分析、行動金融服務及其資訊系統架構、網路安全議題、資訊風險管理、及檢查人員應關注之監理重點，並提供個案分組討論，各國金融監理人員藉此個案研討機會分享監理實務經驗。

本會此次派員赴美國芝加哥參加研討會，一方面增進檢查人員對電子銀行/行動銀行資訊系統與相關科技營運風險之檢查專業知識，另一方面希冀藉由參加此類國際研討會，加強與會各國金融監理人員交流分享檢查經驗，藉鏡國際監理檢查實務經驗，針對本局現行對金融機構資訊業務實地檢查措施提出強化且具體有效之建議。

目　次

壹、 前言

鑑於當今金融環境之科技複雜性，芝加哥聯邦儲備銀行在 2016 年設計和提供全球中央銀行及監理機構之檢查人員研討會「E-Banking/Mobile Banking」（電子銀行/行動銀行），讓學員參與討論交換意見，借鑒並實踐體驗芝加哥美國聯邦儲備銀行銀行之科技檢查監理技術。

「E-Banking/Mobile Banking」課程是由 S.T.R.E.A.M./Technology 實驗室舉辦， S.T.R.E.A.M./Technology 實驗室是由芝加哥聯邦儲備銀行建置，實驗室配備了金融應用系統和電腦作業系統之軟硬體，所有課程項目都是由 S.T.R.E.A.M./Technology 實驗室經驗豐富之專家，分享他們的檢查經驗，透過目前最迫切的監理知識案例，學員間互相研究、練習及團隊合作，讓全球各國 IT（資訊科技）檢查人員互相分享金融科技監理技術。

本篇報告第一部分為「出席研討會目的」，說明主辦單位舉辦研討會之目的及本會派員出席擬達成之成效。第二部分為「研討會過程」，簡述授課講師、參加學員、授課內容與方式。第三部分為「研討內容」，整理本次研討會主要內容，摘要進行說明。第四部分為「心得與建議」，說明參加本次研討會之心得與建議。

貳、研討會目的

本次「E-Banking/Mobile Banking」主要由美國芝加哥聯邦準備銀行之資深 IT 檢查人員擔任講師，本次課程之特色是以電子銀行（網路銀行）和行動銀行之技術和風險為主軸，主題包括電子銀行/行動金融服務技術概論、常見的網路安全威脅和漏洞、Web 伺服器測試、網路身分認證及 Web 應用程式測試，實機測試(Lab 課程)則包括網站的安全評估、漏洞測試和 SQL 隱碼攻擊（SQL Injection），以及如何評估及控制管理上開資訊科技風險。

本研討會對學員的學經歷背景只要求有 IT 檢查經驗一年以上即可，不須一定要在大學研究所是唸 IT 相關科系出身。學員須了解電子銀行/行動銀行基本技術和風險，並且能夠應用這些知識來解決網路安全威脅，建立如何評估電子銀行/行動銀行之新興技術和風險，研討會預期學員能夠完成下列目標:

(一) 電子銀行/行動銀行的技術架構基本概念

(二) 電子銀行/行動銀行解決方案之風險評估

(三) 電子銀行/行動銀行伺服器測試控制

(四) 提出可能的解決方案/程序，以提高電子銀行/行動銀行的資訊安全控制

(五) 評估委外廠商之管理程序是否符合金融機構的政策和標準之要求和控制

此外，學員須能夠瞭解電子銀行/行動銀行之應用系統架構，包含使用者界面邏輯(Presentation Logic)、商業資料處理(Business Logic)和資料存取邏輯(Data Access Logic)，用以描述電子銀行/行動銀行網

站平台之技術及相關風險，並探索 Web 的應用程式測試方法和工具的重要性，並識別各種 Web 伺服器技術相關風險，對相關的網路漏洞和攻擊，提出風險緩解之各種技術解決方案。

資深檢查人員並透過個案研討方式，與會人員就電子銀行/行動銀行風險，藉由分組討論模擬案例所發現之科技風險，進而對金融機構之 IT 科技風險進行評估、控制及緩解，以培養檢查人員風險監控管理之能力。

本次奉派赴美國芝加哥參加研討會，一方面增進電子銀行/行動銀行資訊系統與相關之科技營運風險檢查專業知識，另一方面希冀藉由參加此類國際研討會，加強與會各國金融監理人員交流分享檢查經驗，藉鏡國際監理檢查實務經驗，針對本局現行對金融機構資訊業務實地檢查措施提出強化且具體有效建議。

參、研討會過程

一、會議講師與出席人員

本次授課講師共 5 位，係由美國芝加哥聯邦準備銀行 STREAM 資深檢查人員擔任，包括 Mr. Aaron Cohen、Ms. Carlos Garcia、Mr. Jerald Garner、Mr. William Oei 及 Ms.Sandra Rolnicki ，分別在資訊技術與作業風險管理具備專業豐富之檢查經驗。

參與本次研討會之國家包括來自美國、印度、香港、巴西、南韓、亞美尼亞及俄羅斯及我國等 8 個國家之 24 位金融監理機關人員。

二、課程進行流程

(一)6 月 20 日：本日為下午之半天課程，下午由各國參加研討會之學員辦理報到，於開幕致詞後及學員自我簡介後，隨即開始課程，由於是課程第一天，講師主要簡介一週課程內容，並講授行動金融服務概論(Mobile Financial Services)及其資訊系統架構。

(二)6 月 21 日：上午介紹 IT 檢查之重要議題及如何利用網際網路收集 IT 檢查之重要資訊;下午介紹身分認證技術之應用及 Web 應用程式測試，實機測試課程則為 SQL 資料隱碼攻擊（SQL injection）。

(三)6 月 22 日：上午主要探討資訊安全管理相關議題，包括委外廠商管理及威脅來源、漏洞及修補之變更管理；下午則是資訊安全風險評估及管理，實機測試課程則為 Web IIS 及 Apache 伺服器等。

(四)6 月 23 日：上午就電子銀行/行動銀行(E-Banking/Mobile Banking)

趨勢分析及探討「帶自己的行動裝置來上班(Bring Your Own Device，BYOD)」之相關風險，下午則由講師介紹網路弱點概念及並探討相關風險，實機測試課程則為常見網頁弱點測試(Common Web Vulnerabilities)等。

(五)6 月 24 日：本日為上午之半天課程，上午由講師以個案研討方式介紹如何辨識及分析科技風險，並由學員分組就個案之 IT 風險之監理檢查進行討論及分組簡報後，由資深檢查人員進行案例解答，最後致閉幕詞及頒發結業證書。

詳細課程模組介紹如下：

課程模組	學習目標
電子銀行/行動銀行簡介	• 電子銀行/行動銀行的基本了解
行動金融服務概論	• 如行動銀行、行動支付和替代交易通道(Channel）的各種行動服務概論
識別和分析風險	• 了解與評估電子銀行/行動銀行之相關風險
電子銀行/行動銀行主要組件	• 定義電子銀行/行動銀行 • 電子銀行/行動銀行的基礎設施和組件。
收集信息	• 攻擊者如何獲得一個網站之相關技術資訊
網絡搜索	• 在網際網路之收集有關金融機構 IT 檢查之重要資訊
網絡伺服器	• IIS Web 服務器及 Apache Web 伺服器
Web 驗證/行動設備身份驗證	• 說明網絡身分驗證方法與技術
漏洞	• 演示在網絡伺服器和應用程式常見漏洞 • 說明社交工程攻擊

課程模組	學習目標
使用 SQL	• 結構化查詢語言（SQL）介紹 • 使用 SQL 查看在資料庫中新增、更改或修改資料命令
SQL 隱碼注入攻擊	• SQL **隱碼注入攻擊**取得非法資料
Web 應用程式漏洞測試	• **應用程式**漏洞檢測
委外廠商管理	• 委外廠商的遴選與評估 • 電子銀行/行動銀行的第三方解決方案與監控 • 委外廠商的重大異常事件管理方案
電子銀行/行動銀行發展趨勢觀察	• 電子銀行/行動銀行的新興趨勢與未來發展方向

肆、 研討主題

電子銀行/行動銀行為金融與科技結合的資訊系統，使過去必須跑銀行方能存錢、理財、支付、繳費、貸款等金融業務，只要在電腦和行動裝置上操作，不用透過銀行就能完成大部分之金融業務，金融經營環境日趨科技化，而電子銀行/行動銀行之資訊系統複雜性及風險也伴隨而升高，因此金融機構的電子銀行/行動銀行之資訊系統必須建立良好的安全控制以確保系統正常運作，服務金融客戶以發揮其電子通路功能，並有效降低資訊作業各項風險可能帶來的影響或損失。

本次訓練課程係以電子銀行/行動銀行的技術基礎為主軸，探討資訊科技風險與檢查相關議題，以下謹就課程重點內容摘要說明如下：

一、電子銀行/行動銀行趨勢分析

(一) 趨勢資料分析

1.據研究機構 Gartner 估計，2016 年行動支付交易金額將飆升至$ 7210 億美元，與 2013 年交易金額相較，超過 200%成長速度，而電子銀行的成本比分行臨櫃交易少 99%，行動(手機)銀行的成本也比分行臨櫃交易少 90%。

2. Javelin Strategy & Research：2014 年有 6300 萬美國人使用行動設備支付$ 950 億美元的帳單。

3.美國銀行(BOA)在 2014 年之存款有 10%是通過行動設備裝置轉入。摩根大通銀行(Chase)亦提出報告， 2010 年其客戶的家庭僅 14%使用行動金融服務，於 2013 年，其客戶的家庭已達 41%使用行動金融服

務。

4.美國銀行(BOA)計劃關閉其 20%的傳統實體分行網絡，已經在過去 4 年裡減少了 950 家分行機構(或 15.5%)，在 2014 年又削減約 150 多家，而削減傳統實體分行網絡的同時，每年花費$ 30 億美元，用以提高其行動銀行業務之相關技術和基礎設施。另外美國大銀行花旗銀行(Citi)及摩根大通(JP Morgan)等都紛紛計劃裁減實體分行數量。

5.若依據摩根大通銀行(Chase)的統計，行動銀行每筆存提款的交易成本在該行約每筆交易 3 美分，而若採傳統之櫃員交易則高達 65 美分。

6.用戶分析

(1)美國銀行：3,260 萬人次使用網路銀行/ 1,960 萬人次使用行動銀行

(2)摩根大通銀行：1860 萬人次使用網路銀行/ 2,380 萬人次使用行動銀行

(3)威爾斯銀行：2,720 萬人次使用網路銀行/1,770 萬人次使用行動銀行

(4)美國銀行：行動銀行是增長最快的交易通路，客戶平均比網路銀行年輕 10 歲。

7.美國銀行家對風險趨勢之觀察，提出 2015 年須將網絡安全風險及委外廠商管理視為當務之急，為首要風險管理議題。

(二)銀行未來新趨勢

1.數位銀行

2.數位支付：(1)蘋果支付(Apple Pay)(2)三星支付(Samsung Pay)(3)谷歌錢包(Google Wallet)(4)Paypal(5)近距離通訊支付 Near Field Communication (NFC)

3.建置微分行(Micro-Branches)，配置如下：

(1)網路銀行中心(2)先進的自動取款機(Advanced ATMs) (3)無線網絡(4)咖啡吧(Coffee Bar)

(三)行動銀行(或稱手機銀行)將以下列產品的型式出現：

1.近距離通訊支付 Near Field Communications (NFC)

NFC（Near Field Communication）是一種短距離的高頻無線通訊技術，可以讓裝置進行非接觸式點對點資料傳輸，也允許裝置讀取包含產品資訊的近距離無線通訊 (NFC) 標籤，可用於付款、購買交通車票或活動門票、門禁管理及資料通訊交換等應用上，藉由 NFC 的技術建置於智慧型手機上，將使其能夠成為行動支付之電子錢包。

2.Visa 卡個人支付 Visa Personal Payments (P2P)

Visa 卡個人支付全球通匯，直接匯款到全球各地符合資格的 Visa 信用卡、Visa 金融卡及 Visa 電子錢(禮物卡)帳戶。Visa 全球通匯服務的單次匯款金額上限為 2,500 美元，只要 30 分鐘到一個工作天，就可以透過網路銀行、行動銀行、ATM 或分行臨櫃等各種管道跨國通匯。

3.萬事達卡發送 MastercardSend

萬事達卡的 MasterCard Send 平台所推出類似 Visa 卡個人支付（Visa Personal Payments）之個人支付服務，幫助商家向消費者匯款，且無需擔心是否擁有銀行賬戶，也不受地理位置的限制。保險理賠、退款、電子支付、社會保險和退稅可以現時轉賬，直接傳輸發送到銀行帳戶中，幾乎任何美國金融卡帳戶，包括非萬事達卡，都可以進行轉帳付款，該服務也包含跨境 P2P 支付功能。

4.谷歌買入 Google “Buy”

谷歌通過增強 Google Shopping 服務功能提升其電子商務服務，與亞馬遜展開直接競爭，谷歌與零售商建立一個「買入」 按鈕以便於用戶使用谷歌在線購物服務，可隨即按鈕買入，與亞馬遜具的「一點通（one-click ordering）」功能相似。

5.GoBank 虛擬的銀行賬戶

美國一家虛擬網路銀行 Green Dot (綠點銀行)，發行一個專門為智慧型手機使用的銀行帳戶，稱作 GoBank，申請帳戶時，用戶只要透過手機便可以登入行動版的網頁或是直接下載行動軟體進行設定，就可以快速完成帳戶設定，其銀行主要有許多一般大銀行沒有的特色和服務，包括匯錢給親朋好友時是免手續費，且可以透過電子郵件和簡訊或甚至是 Facebook 的通知功能就可完成。此銀行為虛擬網路銀行，所以沒有任何的實體銀行，假如要存錢，除了可以至有收取現金的 ATM 外，GoBank 還與大型超市 Wal-Mart 合作，讓用戶也可以在超市存錢，假如要提款，也可以利用實體的提款卡至一般的 ATM 提取現金，最大的好處是沒有任何跨行提款的手續費。

6.無卡取款手機錢包（FIS Mobile Wallet with Cardless Cash）

無卡取款用戶可以使用自己的智慧手機於 ATM 提取現金，通過手機應用程式來驗證帳戶，也可用 QR 碼掃描完成交易。

7.遠端存款 Remote Deposit Capture

不用親自到銀行存入支票或使用自動提款機(ATM)，只要用手機將支票照幾張像，就可以輕鬆把錢存入銀行，對支票拍照時，接收影像的電腦會尋找金額、支票號碼、支票底部的數字、開票人帳戶資訊、

以及銀行的代碼等，也會核對支票背後是否有受款人的簽名。銀行及票據交換所據此安排票款從開票人帳戶入受款人帳戶的程序，也防止相同的支票被多次存入銀行。

（四）詐欺防範

1.鑑於網絡安全之威脅所發生之頻率和複雜性不斷增大，造成監理單位和市場的壓力，因此全球金融機構防範網路詐欺，必須投入大量的時間和資源，以適當抵禦惡意程式和先進的網路詐欺威脅，所以必須建置全面的網路詐欺監測架構，靈活部署以監控用戶群體和多種電子存取通道之交易。

2.各種類型的網路攻擊

攻擊有很多種方法，但最終的目的就是從啟動客戶現金管理帳戶中取走客戶的金錢，各種類型的網路攻擊簡介如下：

(1)**瀏覽器中間人攻擊 (Man-in-the-browser)**

使用木馬程式侵入使用者電腦中，該程式會利用電腦上的瀏覽器攔截所有輸入或呈現的資訊。

(2)**中間人攻擊（ Man in the Middle）**

攻擊者在訊息傳送時，於發送者和接收者之間暗中讀取、插入及更改訊息，從中竊取相關的客戶或帳務重要資訊，中間人攻擊偏重在實體網路上，也可以透過無線基地台或是入侵網域名稱伺服器等方式，讓資料轉向送至駭客的主機上。

(3)**按鍵記錄 (Key Logging)**

按鍵記錄利用木馬程式記錄個人在電子郵件之登錄訊息、社交網

站和網路銀行帳戶，按鍵記錄攻擊可以通過網頁感染的方式，並且可以用各種方式來偽裝。

(4)**連線劫持 (Session Hijacking)**

利用 SessionID 以 Cookie 方式存到使用者端電腦的特性，竊取存在使用者端電腦的 SessionID，再冒用網頁使用者的身份進入該使用者所使用的網站竊取重要的個人金融資訊。

(5)**網址嫁接（Pharming）**

藉由入侵使用者電腦、植入木馬程式(Trojan)，或者是利用域名伺服器(Domain Name Server；DNS Server)的漏洞，將使用者錯誤地引導至偽造的網站中，並伺機竊取重要資料，一般使用者通常會認為自己所瀏覽是自己熟悉信賴的網站，但不知不覺間被重新導向傳送至惡意網站，而將自己機密資料洩漏。

(6)**釣魚網站 (Phishing)**

釣魚網站是利用詐騙或誘拐方式將使用者導向看似合法的網站，誘使使用者在惡意網站中輸入各項個人資料，而由此取得可利用的客戶相關金融資訊。

(7) **SQL 資料隱碼攻擊 (SQL Injection)**

在 Web 應用程式時，如果沒有對使用者的輸入資料做妥善的過濾與處理，即可利用驗證設計上的疏失進行攻擊，程式可將使用者輸入的內容組合成查詢的指令，傳送給資料庫伺服器執行；若使用者輸入之資料中含有某些對資料庫系統有特殊意義的符號或命令時，便可能讓使用者對資料庫系統下達指令，因而造成資料庫遭竊取資料。

(8)跨站腳本攻擊 Cross-Site Scripting(XSS)

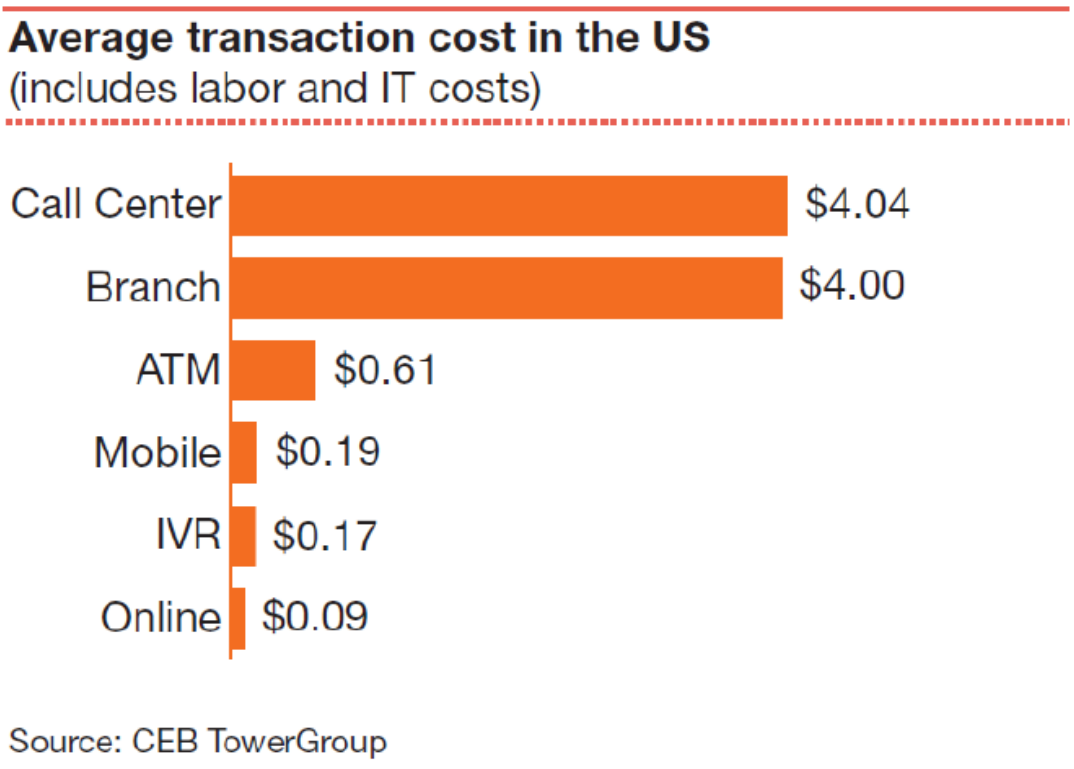
利用網站上允許使用者輸入字元或字串的欄位插入 HTML 與 Script 語言，造成其他正常使用者在觀看網頁的同時，瀏覽器會主動下載並執行部份惡意的程式碼，或被導入至惡意網站。

二、行動金融服務概論(Mobile Financial Services)及其資訊系統架構

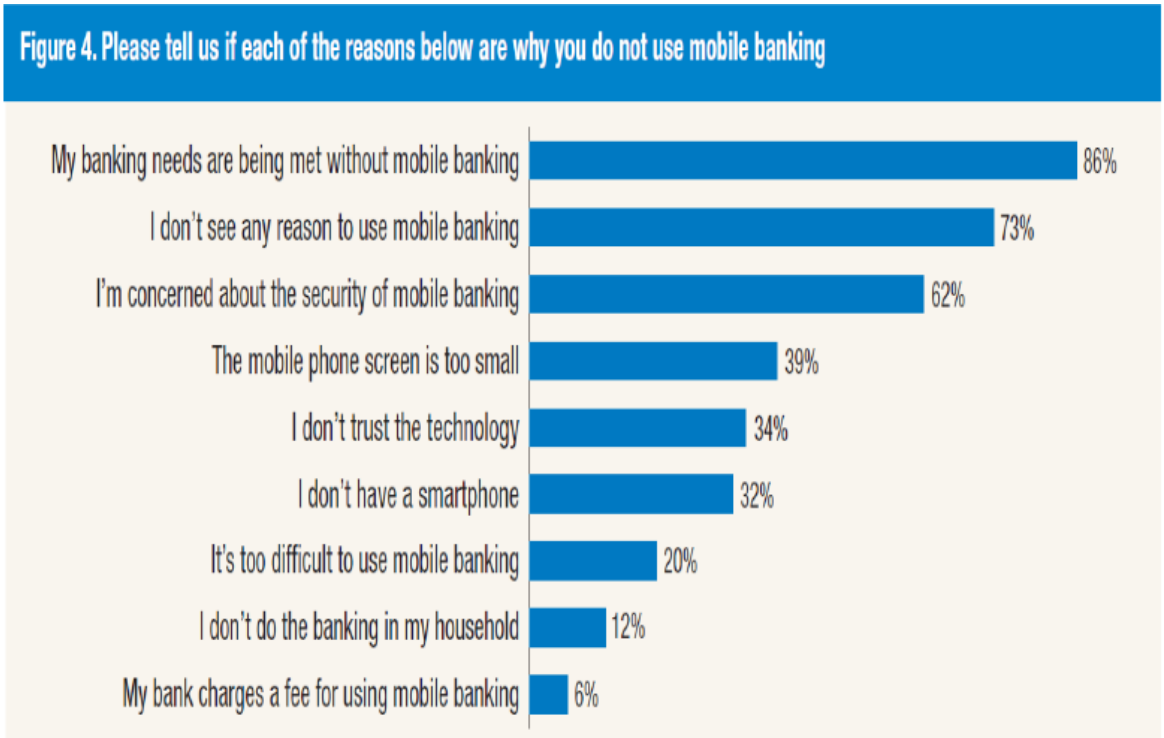
(一) 行動金融服務概論(Mobile Financial Services)

1.**為何銀行要推展電子銀行/行動銀行業務**

可從交易成本及客戶認知兩方面分析，美國銀行之交易成本分析如下圖，可知建置分行作業人員，每筆交易的成本達$4.00 美元，客服中心的成本一樣不便宜，達$4.04 美元;惟完成同樣的一筆交易，ATM 僅需$0.61 美元，行動銀行僅需 0.19 美元(約分行作業人員成本的 1/6)，網路銀行更低，僅需 0.09 美元(約分行作業人員成本的 1/44)，因此隨著社會大眾普遍資訊素養的提昇及 3C 產品的普及，尤其是年輕族群對電子銀行/行動銀行的接受度很高，銀行推展電子銀行/行動銀行有助於降低分行作業成本。

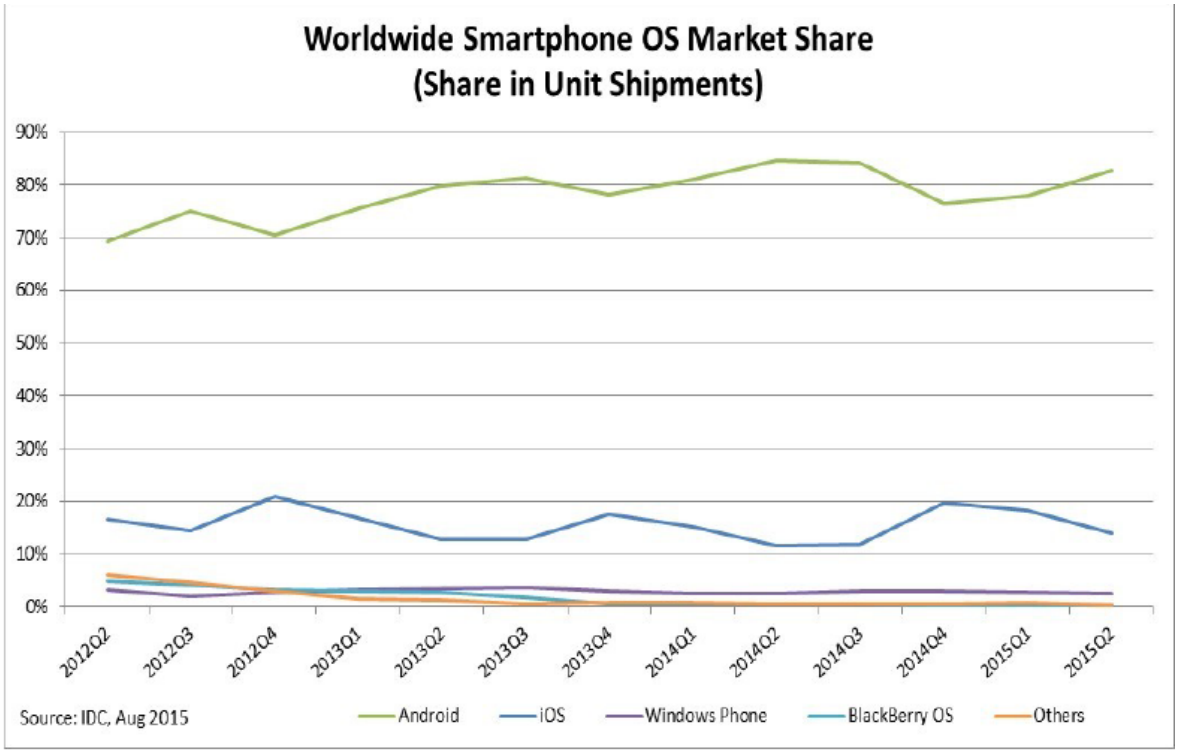


銀行客戶目前對行動銀行最大的疑慮，仍是來自於對行動銀行安全性的質疑，高達 62%。



2.各種智慧型手機平台占有率的比較

全球智慧型手機市場分佈情形如下圖所示，**截至 2015 年 6 月 (2015Q2)，谷歌的 Android 佔約 82%，蘋果的 iOS 佔約 13%**及其他諸如 RIM 的黑莓操作系統、 微軟的 Windows Mobile（Phone）、Samsung 的 Bada 及 Nokia 的 Maemo 等合佔約 5%。就不同的作業系統平台，其行動銀行之操作介面及應用系統風險亦不同，檢查人員須依不同作業系統平台之風險程度進行查核。



(二) 行動金融服務資訊系統架構

1.行動金融結構組件

(1)客戶端：手機 APP 及 IE、火狐(Firefox)及 Chrome 等瀏覽器。

(2)傳輸協定：SSL /TLS, HTML, HTML5

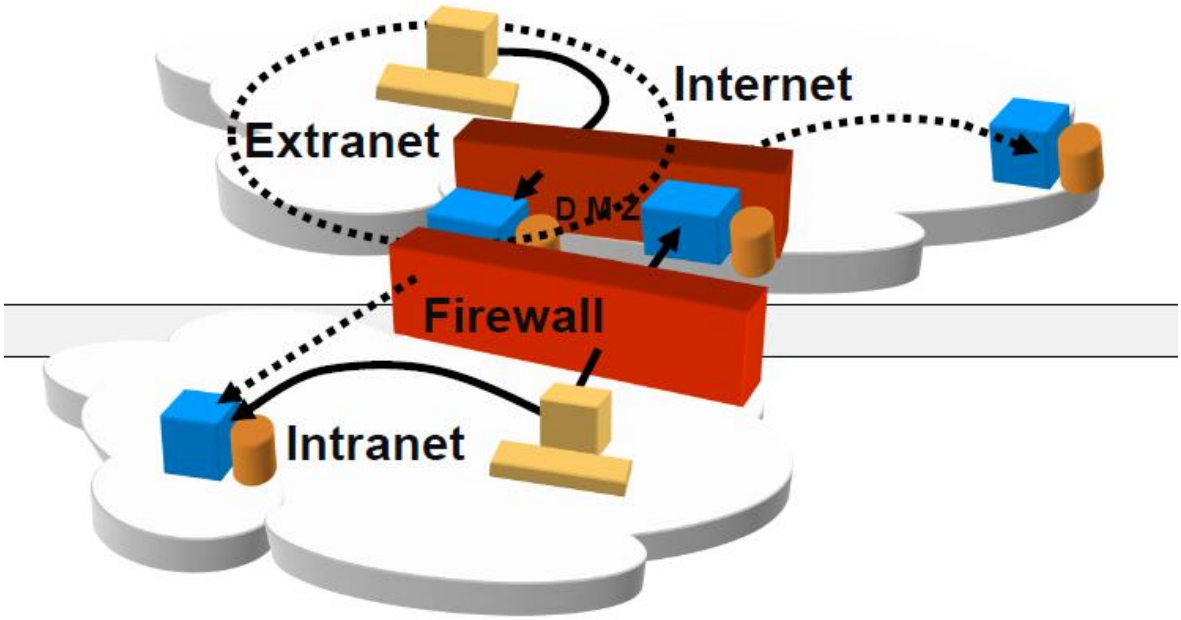
(3)Web 伺服器：IIS, Apache

(4)應用程式碼：Perl, CGI, PHP, JSP, ASP, Python 和 Ruby 等

(5)資料庫：Oracle, MySQL, SQL Server, DB2

2.網路架構與安全基礎設施

(1)網絡：區分為內網及外網，基本上以防火牆區隔外網(Extranet)、內網(Intranet)及非軍事區(DMZ)區。



(2)交換器(Switches)

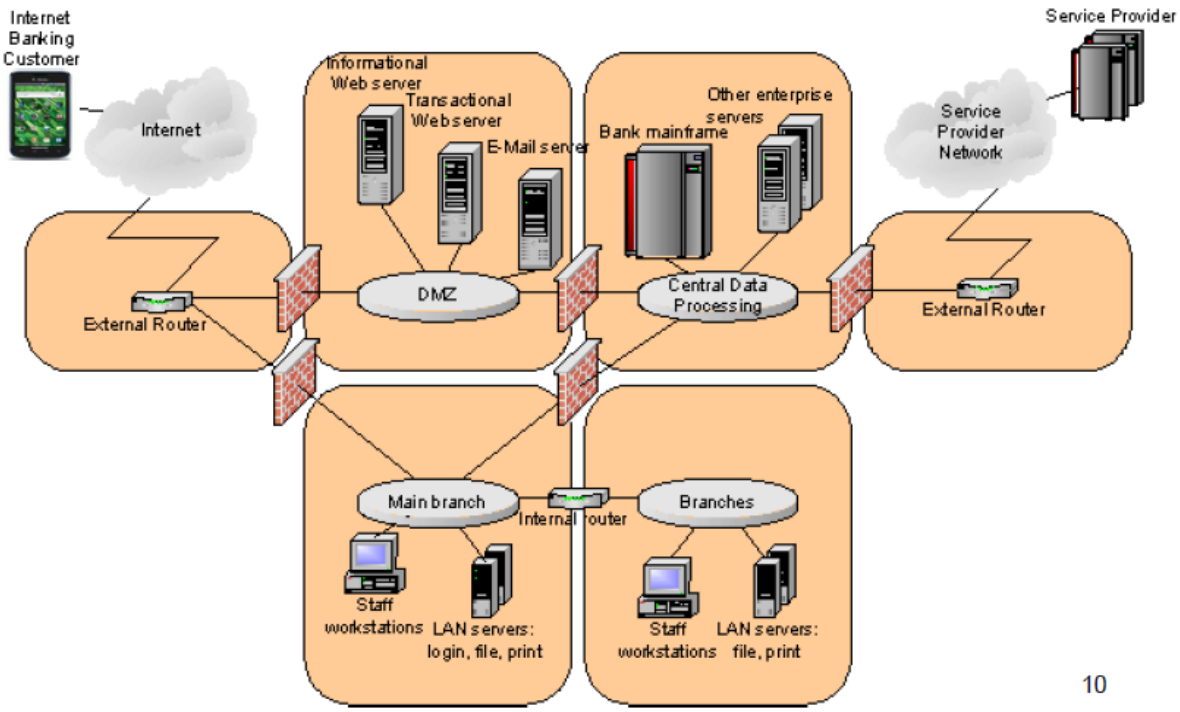
(3)路由器

(4)防火牆

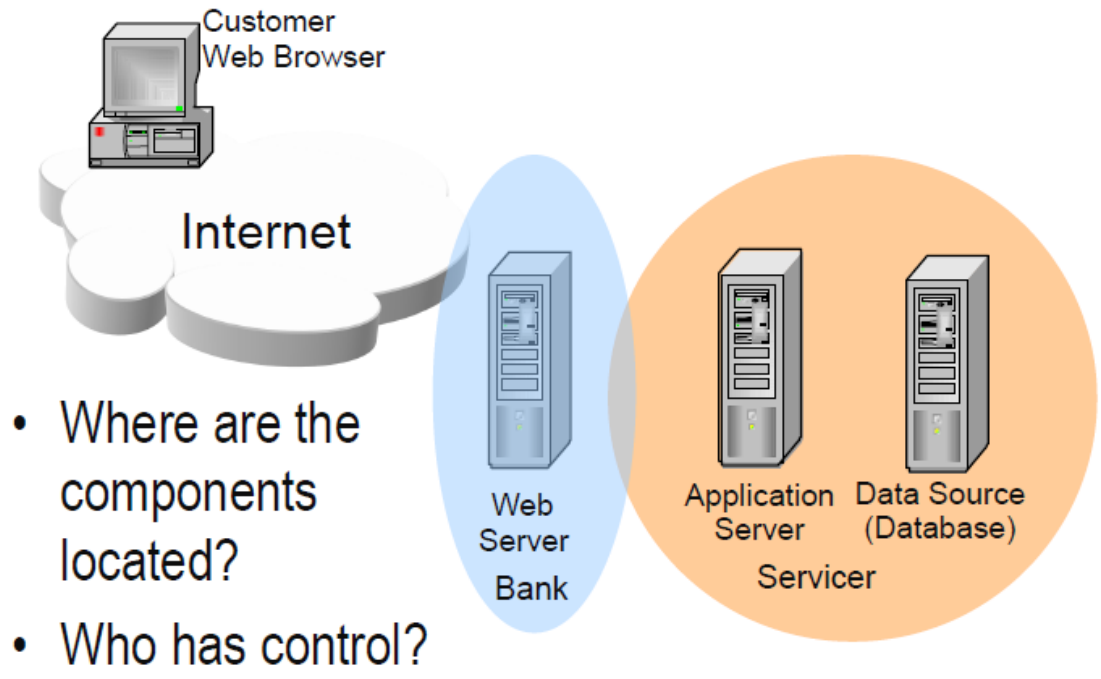
(5)入侵偵測和防禦系統（IDPS）

(6)非軍事區 Demilitarized Zone (DMZ)

整體架構圖如下所示：

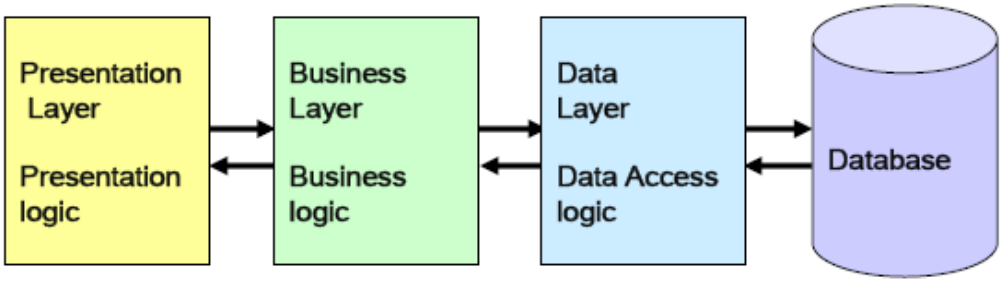


網路攻擊的風險等級區分，可大約以運行有多少連線電腦、應用程式的平均數目及潛在使用者數等因子(factor)作估計，估計後，基本之安全檢核須了解上開設備之實際位置和由誰控制，如下圖所示：



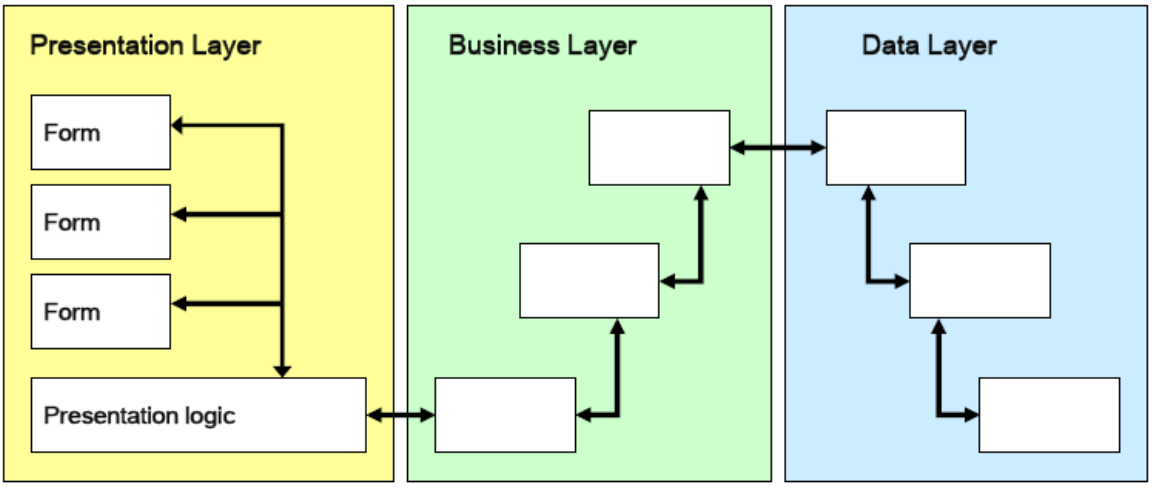
3.應用系統架構

應用系統架構包含了使用者界面邏輯(Presentation Logic)、商業資料處理(Business Logic)和資料存取邏輯(Data Access Logic)，如下圖所示：

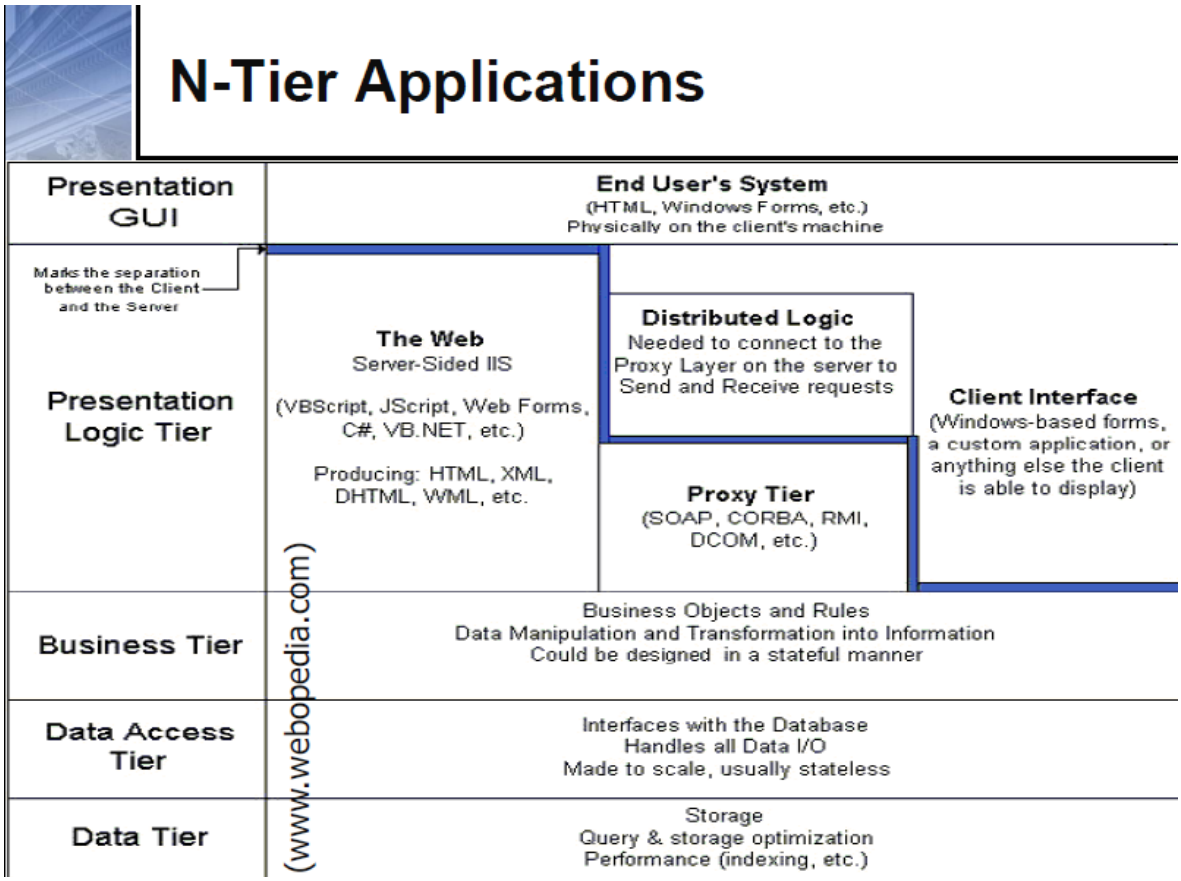


- 使用者界面邏輯:將資料呈現給使用者，並接受使用者更改資料輸入
- 商業資料處理邏輯:允許執行資料驗證和傳送相關資料到資料庫
- 資料存取邏輯:可以在不同資料庫系統之間發送和接收來自資料庫的資料。

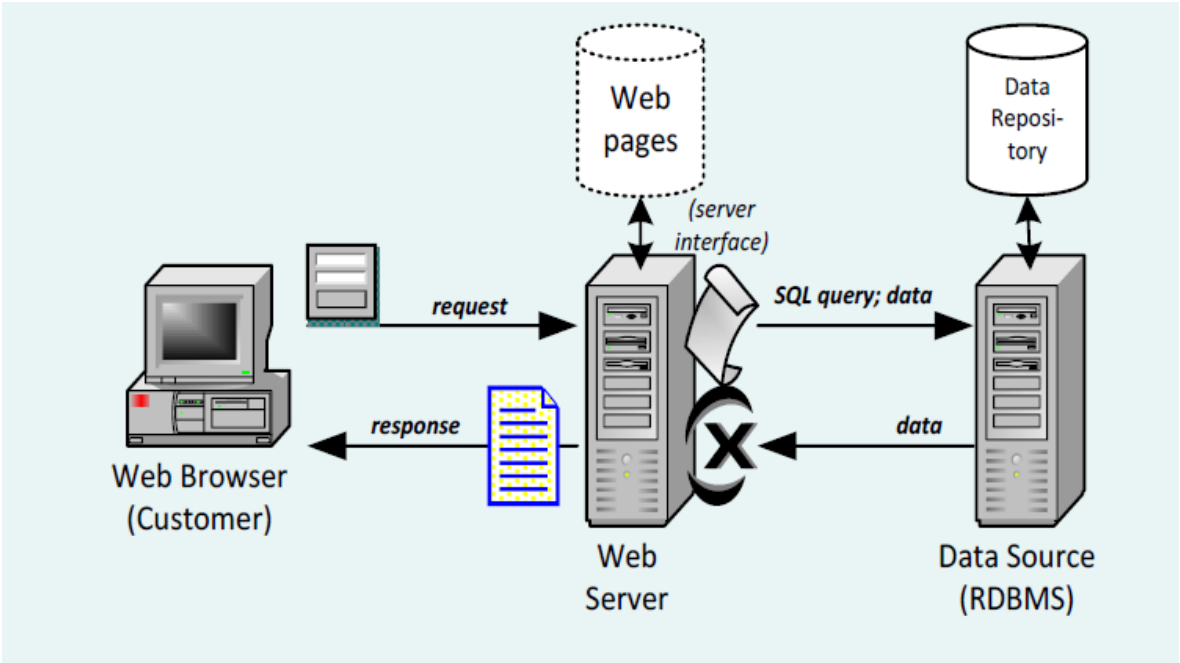
技術上對應可以再細分為 1 層應用程式、2 層應用程式及 3 層應用程式架構，乃至 N 層應用程式架構(使用不同的平台，例如：Python 和 PHP 和 Ruby，SQL，Oracle 等)，如下圖所示：



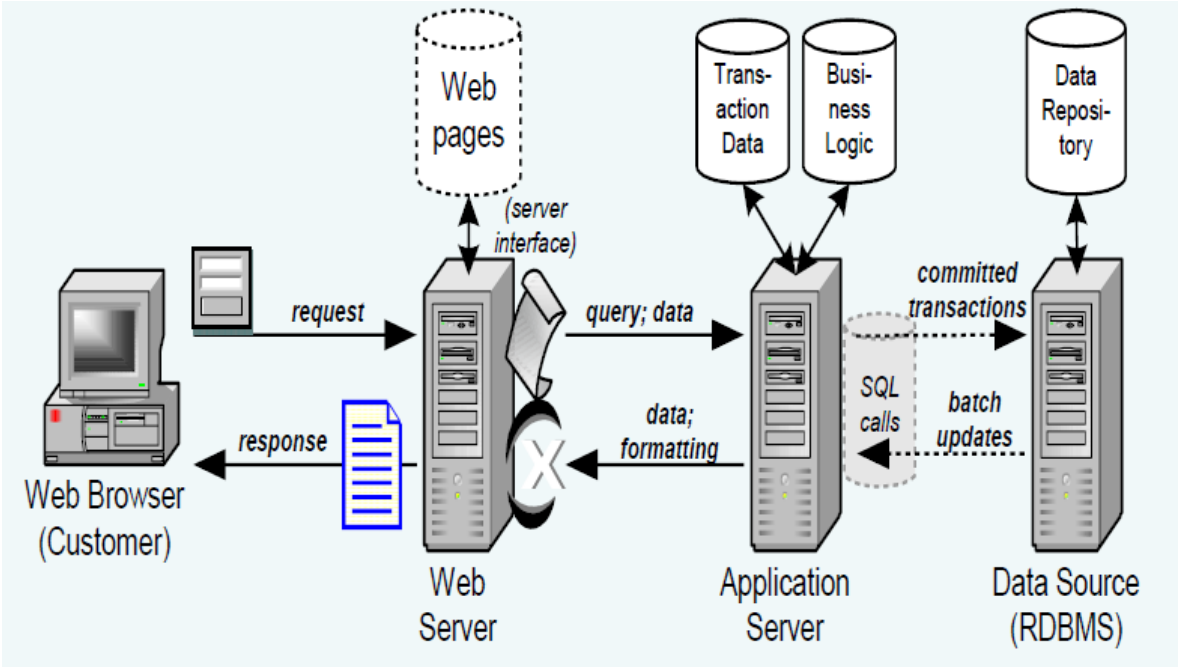
對應的實作架構如下圖：



在我國最常用者為 2 層應用程式及 3 層應用程式架構，圖示如下：



2 層應用程式架構示意圖



3 層應用程式架構示意圖

4.資料庫結構化查詢語言 SQL

(1) 結構化查詢語言（Structural Query Language， SQL），是一種特殊目的之程式語言，用於資料庫中的資料查詢語言，有 4 個基本命令：

- 選擇（Select）-選擇記錄
- 刪除（Delete）-刪除記錄
- 更新（Update）-更改記錄
- 插入（Insert）-添加一條記錄
- 指定表格用 FROM 指令，應用的條件則為 WHERE 指令

(2)基礎範例如下：

Example:

SELECT * FROM Account_Table WHERE UserID= ‘123’

- * -wildcard that indicates retrieve all columns in the table
- FROM Account_Table -retrieve field from this table
- WHERE UserID= ‘123’ -retrieve the record associated with a UserID of

123

(3)開發人員都會以字串組合的方式建立 SQL 指令，而由於 SQL 指令語法會依照特定條件，因此讓駭客有機會利用 SQL 的組合方式進行攻擊，讓資料庫的資料或實體伺服器被破壞，導致服務中斷或是系統癱瘓等後果，或是以邏輯的漏洞，如在密碼欄寫入特殊字串(例如' or '1'='1’)，讓該字串形成的邏輯判斷永遠為真，而不需要知道密碼，以達成非法登入系統的目的，此種攻擊手法稱為 SQL 注入隱碼攻擊（SQL injection）。

三、電子銀行/行動銀行資訊安全議題

(一)身分驗證

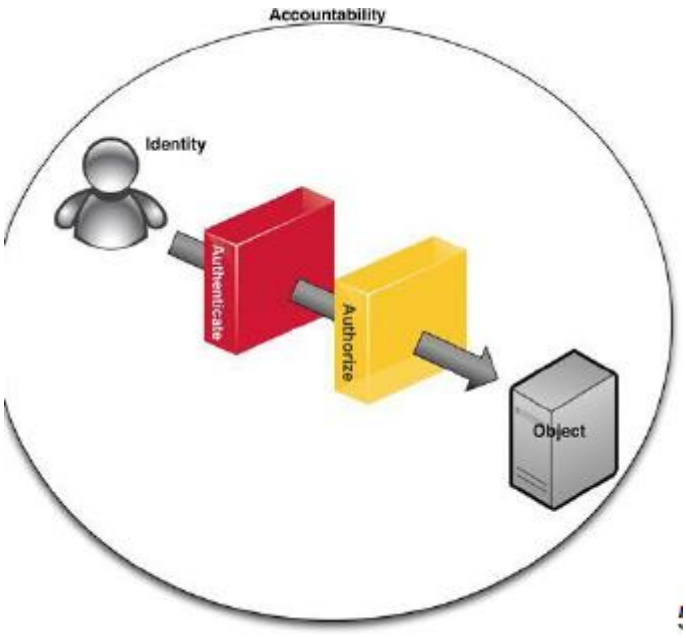
1.驗證 vs. 授權 vs. 可靠性

(1)驗證

檢核一個人與他聲稱是誰是否相符，通常使用多因素認證來達成身分驗證目的。

(2)授權是決定什麼樣的資源可以被使用者存取。

(3)可靠性指從身份識別(identification)通過身分驗證和授權記錄。



2. **驗證類型**

(1)你所知道的東西（Something you KNOW ），如：PIN、密碼、帳號及使用者名稱(User ID)。

(2)你擁有的東西（Something you HAVE）

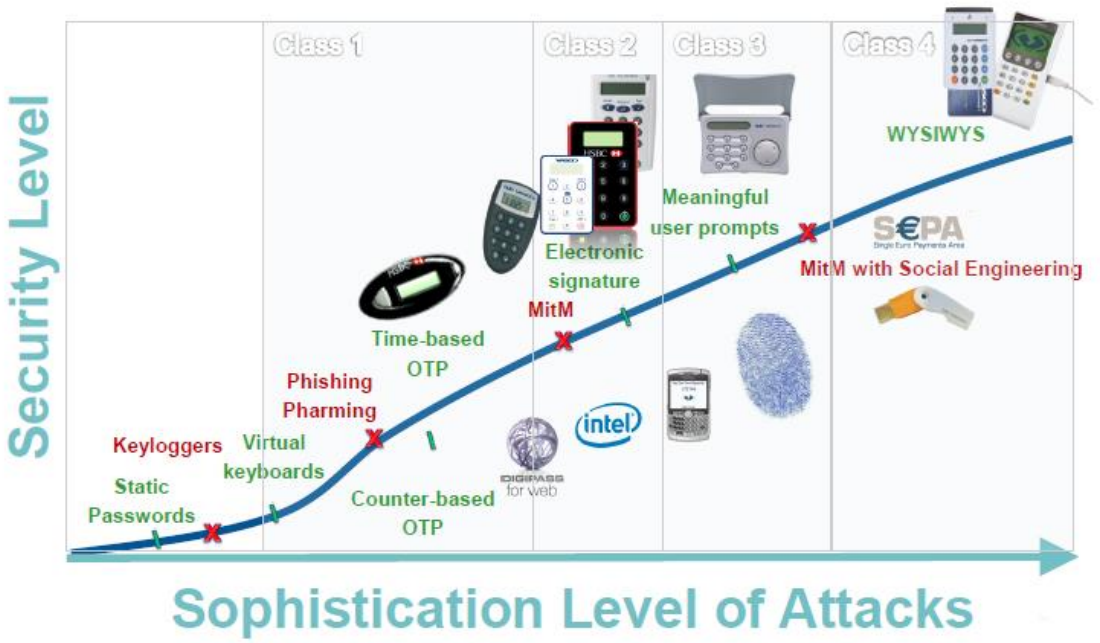
代碼器(Token)、SecureID、卡片及智慧卡。

(3)你本身（Something you ARE） ：生物識別技術，如：指紋及虹膜等。

(4)單因素和多因素身份驗證

一個因素認證涉及上面其中一種方式，二因素認證則涉及上面兩個方式，多因素認證涉及多個以上方式。

下圖顯示隨著攻擊演進的複雜度，伴隨而生的驗證類型：



3.驗證機制之穩健實務做法

(1) 新客戶需要較強的驗證機制

- 從受信任的第三方驗證

- 邏輯驗證（來源之間的資料須一致）
- 核實客戶是否有欺詐行為的任何記錄
- 程序性控制首次開戶帳戶

(2)身分驗證應該產生稽核日誌

- 不尋常的登入活動
- 入侵檢測
- 促進每個人對自己驗證機制的保管責任

(3)定期監測和報告機制以快速檢測異常活動

(4)強身分驗證則需要多因素驗證機制的組合，而不是只依靠一個因素

4.檢查實務要點

(1)電子銀行/行動銀行需要多因素驗證

(2)所有的系統需制訂密碼政策並落實

(3)在一個持續的基礎，評估新的風險，驗證機制須進行適當更新

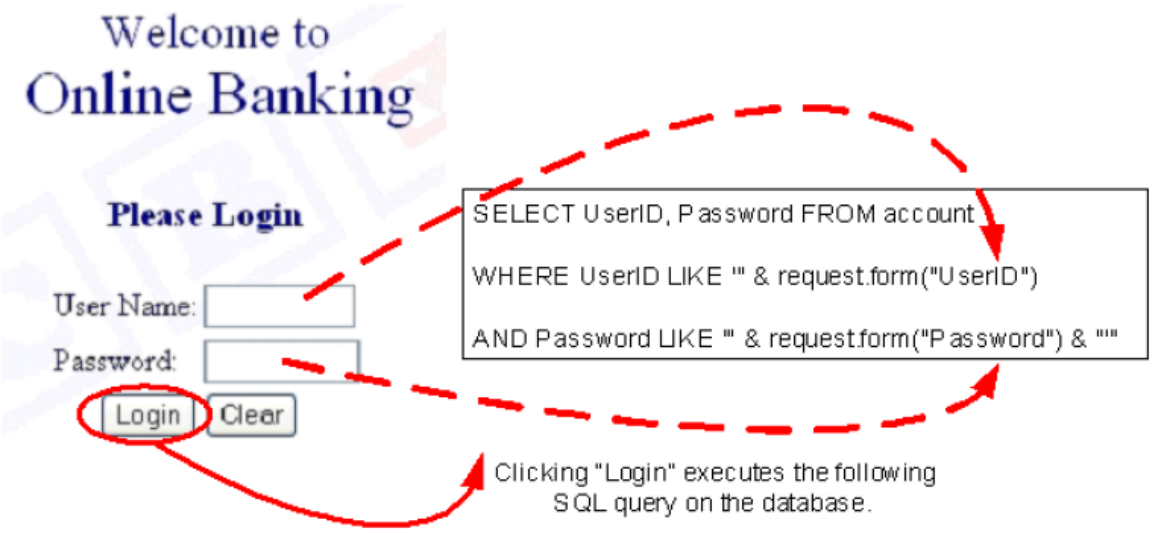
(4)行動銀行另應注意行動裝置是否有越獄或 root？感染病毒？遺失位置？異常使用行為? 如下圖所示:

(二) 網絡漏洞

1.**網絡三大易遭攻擊之漏洞**

(1) SQL 隱碼攻擊（SQL injection）

發生於應用程式之資料庫安全漏洞，在輸入的字串之中夾帶 SQL 指令，程式忽略檢查，夾帶的指令就會被資料庫伺服器誤認為是正常的 SQL 指令而執行，因而遭到破壞或是入侵。



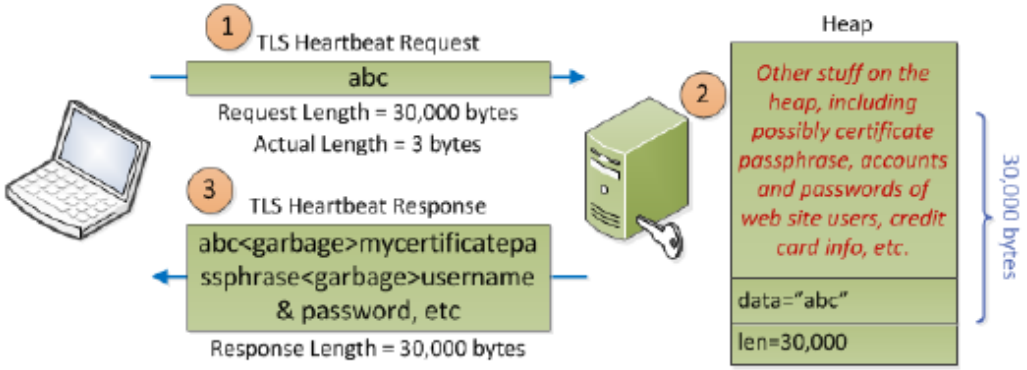
(2)跨網站指令碼（Cross-site scripting，通常簡稱為 XSS）

是一種網站應用程式的安全漏洞攻擊，允許惡意使用者將程式碼注入到網頁上，其他使用者在觀看網頁時就會受到影響。這類攻擊通常包含了 HTML 以及使用者端腳本語言(Script)。

XSS 攻擊利用網頁開發時留下的漏洞，注入惡意指令代碼到網頁，使使用者載入並執行攻擊者惡意製造的網頁程式，攻擊成功後，攻擊者得到更高的權限，執行操作私密網頁、會話和 cookie 等各種內容。這些惡意網頁程式通常是 JavaScript，但也包括 Java，VBScript，ActiveX，Flash 或者甚至是普通的 HTML。

(3)心臟出血漏洞（Heartbleed）

OpenSSL 是一個商業級的軟件工具包，提供使用 SSL 和傳輸層安全（TLS）協議加密。心臟出血漏洞出現在加密程式庫 OpenSSL 之程式錯誤，只要使用存在缺陷的 OpenSSL，無論是伺服器還是使用者端，都可能因此而受到攻擊，原因是實作 TLS 的擴充功能時沒有對輸入進行適當驗證（缺少邊界檢查），即可以讀取的資料比應該允許讀取的還多。



3.網路安全漏洞對金融機構和客戶之風險

(1)該漏洞可能影響許多安全的 Web 應用程式和服務

(2)任何漏洞的應用程式或服務可能完全破壞金融機構使用的資訊系統

(3)加密密鑰、認證證書(authentication credentials)和機密訊息目前暴露在

網際網路的量是巨大未知的。

(4)修補漏洞是複雜的(成千上萬的應用程式),所有金融機構可能需要付出巨大的努力以確定和修復漏洞,金融機構應建立妥適的漏洞管理程序,包括訂定管理政策、漏洞風險評估及採行適當的系統漏洞修補期限及措施。

(5)規模較小的金融機構可能面臨更大的風險,因為漏洞的複雜性和自身對服務委外廠商有較高的依賴性。

(6)由於傳統媒體、網路及社交媒體的關注報導,客戶也認知到網路漏洞的安全風險,造成金融機構的聲譽風險。

(三)帶自己的行動裝置來上班(Bring Your Own Device,BYOD)

1. BYOD

指允許員工將智慧型手機或平板電腦帶到辦公場所,直接連接公司內部網路,存取資料並處理公務,員工自攜行動裝置投入工作,優點是公司節省了採購硬體成本,員工也因使用自己喜歡且熟悉的行動裝置,而提升工作的生產效率,缺點為造成資訊安全控管之難題,因為金融機構勢必得面臨管理多種設備存取資訊系統。

這些員工私人擁有之行動裝置能存取並儲存金融機構的敏感資料,而這類方便性的行動裝置又容易丟失,致金融機構之機敏資料及客戶個資洩露風險大增,BYOD 政策是對員工使用者需求和安全策略必要控制之間的微妙平衡。

2.在 BYOD 之風潮下,本局所查核之部分金融機構確實有開放 BYOD,如:產險業者。金融機構若開放 BYOD,則需建構安全優質的行動應用環境,應就 BYOD 議題進行探討並訂定政策及管理規範,監控網路攻擊及和客戶個人資料之存取。

3.行動裝置控管(Mobile Device Management ,MDM)

(1)MDM 是集中管理行動裝置設備之無線網絡和相關服務,金融機構應針

對 BYOD 訂定行動裝置管理及網路存取控制政策，包括資料儲存與分享、設備連結與授權、照相、影音及資料連結等功能控制及允許所使用之應用程式等。

(2)行動裝置比起桌上型個人電腦更容易丟失或被盜，使資料容易遭毀損盜取或不當存取，為防止金融機構應用程式和資料在行動設備上未經授權的存取，因此須使用 MDM 機制，可以包括密碼保護、硬碟加密和或遠端擦除行動裝置資料技術。

(四）應用程式測試

依據 2009 年 Gartner Group 的研究報告指出，目前的駭客攻擊有 75%都發生在應用系統層面的安全事件，而防火牆、防毒軟體或入侵偵測系統皆無法防禦及修復應用系統安全的漏洞，須從應用系統本身著手分析、測試及強化修補。

1.源碼檢測(原始碼檢測)

(1)源碼檢測可以透過已知弱點特性的比對，針對原始碼的內容進行分析找出其程式中潛藏的安全弱點，分析其弱點種類及攻擊路徑等資訊，透過分析的結果，開發人員可發現程式中的潛在弱點而進行修補。

(2)源碼檢測可以分為人工檢測與自動化檢測，人工檢測的方式以人工目視的方式檢查程式碼，找出程式碼中具有安全威脅的地方；檢測人員必須擁有充足的程式開發及資安知識方才能找出應用程式中漏洞，惟人工程式碼檢測效率不佳且需耗用許多人力與時間。隨著檢測工具的發展，採用自動化原始碼檢測的方式逐漸受到重視，從一開始程式碼的檢測、弱點等級分類至最後報表的產生，都可自動化產生，**惟目前要達到完全自動化來進行檢測仍有許多不足之處，檢測的結果仍會有誤判 (False Positive) 及漏報，因此現今仍是以人工搭配自動化檢測工具來進行程式碼的安全檢測。**

2.滲透測試(Penetration Test)與 OWASP Web 應用程式測試規範

(1)滲透測試是委任受信任的第三方進行評估網路安全的活動，它透過對企業網路進行各種手段的攻擊來找出系統存在的漏洞，進而驗證出網路系統存在安全風險的技術，通常也被稱為黑箱測試。

(2)滲透測試基本上是遠端測試運行的應用程式，滲透測試透過模擬真實攻擊行為，來評估電腦網絡系統安全，滲透測試過程包括對系統的弱點、技術缺陷或漏洞的主動分析並利用安全漏洞攻擊，找出安全問題以證實惡意攻擊者有可能竊取或破壞金融機構的數位資產、資訊與資料。

(3)國際常用的應用程式測試規範有 OWASP Checklist、OWASP ASVS、CWE/SANS Top 25 這幾種。

(4)開放網路軟體安全計畫，簡稱 OWASP（Open Web APPlication Security Project），是一個開放社群之非營利性組織，主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，針對不同的軟體安全問題進行討論與研究。**OWASP 在美國發表關於行動式裝置的十大弱點風險，簡要說明如下：**

M1.不安全的資料儲存(Insecure Data Storage)

指敏感性資料未受到適當的保護，如：敏感性資料未加密或是一些不常用到的暫存資料可能含有敏感訊息(例如：登入帳號與密碼)，可能會造成機密性資料損失、憑證外洩及侵犯隱私等。

M2.弱伺服器端之控制(Weak Server Side Controls)

行動裝置的弱點並非只存在於行動裝置端， APP 應用程式或後台伺服器端(含雲端系統)的程式亦有可能存在弱點。

M3.傳輸層保護不足(Insufficient Transport Layer Protection)

行動裝置於傳輸機敏性資料時，常發生未加密情況，例如：瀏覽器本

身不支援 HTTPS 功能，或是使用的 APP 應用程式未採用加密方式進行資料的傳輸(如：登入系統、交易資料等)，因此可能會造成駭客使用中間人攻擊(Man-in-the middle attacks)，從中竄改或竊取封包資料，進而造成機敏資料洩漏。

M4.客戶端注入(Client Side Injection)

行動裝置網頁應用程式若存有 Injection 弱點，攻擊者仍可利用 SQL Injection 或 XSS 攻擊手法來提升行動裝置的權限。

M5.不足的授權與認證(Poor Authorization and Authentication)

行動裝置的網頁應用程式採用永不變的數值來執行身分驗證與授權，例如：國際行動裝置設備識別碼(International Mobile Equipment Identify Number, IMEI)或通用唯一識別碼(Universally Unique Identifier, UUID)。

M6.不適當的連線會話處理(Improper Session Handling)

為方便使用者存取或使用，行動裝置的應用程式 session 期限設定較長，通常這些 session 經由 HTTP Cookies、Oauth Token、Single Sign-on 等方式來進行維護，若使用裝置的硬體識別碼來當作 session 值，攻擊者很容易猜到 session 內的機密性內容(例如：帳號或密碼)，提升攻擊者的權限而進行非授權的資料存取。

M7.安全決策經由不受信任的輸入(Security Decisions Via Untrusted Inputs)

應用程式可能經由惡意攻擊者精心設計，或是應用程式遭攻擊者透過 Client Side Injection 攻擊方式來消耗行動裝置的硬體資源或提升權限。

M8. 側通道資料洩漏(Side Channel Data Leakage)

Side Channel 是指行動裝置中的第三方應用程式，這些應用程式可能會自動幫使用者儲存一些敏感性資訊，例如：網頁暫存(Web Cache)、按鍵側錄(Keystorke Logging)、擷取畫面(Screenshots)、日誌檔(Logs)或暫存

目錄(Temp Directories)等，一但攻擊者成功取得行動裝置權限時，就導致資料洩漏。

M9. 加密失效(Broken Cryptography)

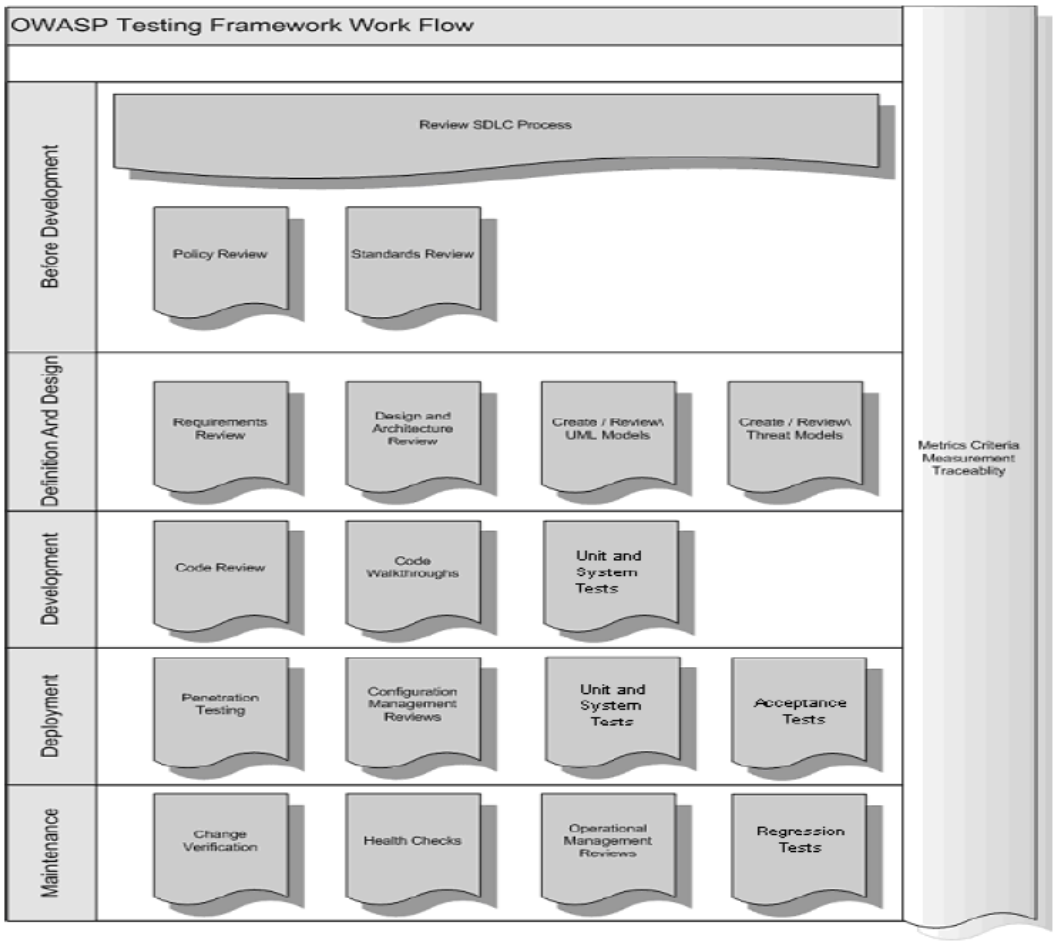
加密失效分為兩種情況，一種是使用強加密演算法卻遭到破解，另一種為使用過於簡單的加密演算法遭到破解。OWASP 提出幾個對於加密方法的謬誤，例如：編碼(Encoding)、混淆(Obfuscation)、序列化(Serialization)，皆非為嚴謹加密方式，攻擊者能輕易破解簡單的加密演算法後，取得行動裝置權限或洩漏機敏資料。

M10. 敏感資訊洩漏(Sensitive Informaiton Disclosure)

指應用程式原始碼中，把輸入或輸出的相關參數直接寫入在程式碼當中，因此只要攻擊者能夠取得應用程式的原始碼，若原始程式碼內容含有敏感資訊，像是 API 金鑰、帳號或密碼等，就可能會造成金融機構個人憑證洩漏。

3.應用系統開發各階段之漏洞安全威脅檢測

應用系統開發各階段所對應之漏洞安全威脅檢測方法，如下圖所示。



設計階段：須依資訊安全政策及開發程序所規定之流程開發。

開發階段：須針對源碼檢測，即對原始碼做安全漏洞掃描，再將發現的安全漏洞依嚴重程度做等級分類，追蹤安全問題及提供修復建議，並有稽核機制做審查及追蹤修復狀況。

測試階段：執行弱點掃描及模擬駭客進行滲透測試以確保測試完整性。

上線維運階段：已上線的應用系統，利用資安設備部署提供防禦功能，監控及追蹤攻擊並定期執行弱點掃描及滲透測試。

(五) 電子銀行/行動銀行委外作業管理

1.隨著金融服務業與資訊科技的快速發展，金融機構仰賴資訊委外作業建置先進的技術，透過有效的委外作業，金融機構使核心業務更專業化及取得較佳的資訊作業方式，資訊委外作業亦有助金融機構強化其特定金

融商品服務的機會。

2. **委外作業風險趨勢**

紐約金融服務部日前發布報告，發現如下：

(1)約 33%銀行未要求他們的第三方廠商，通知他們在資訊安全事件或其他網絡安全漏洞事件。

(2)約 33%銀行之資訊安全需求，須由第三方委外廠商提供解決方案。

(3)約 33%銀行未要求委外廠商揭露其最低限度的資訊安全措施

(4)少於 50%銀行方有進行至少一次之第三方委外廠商的實地查核。

3.**委外作業風險**

一般而言，我國的電子銀行/行動銀行系統前台多委外建置，資訊作業委外作業風險主要來自下列幾類：

(1)法遵風險

委外廠商（受託機構）的服務、產品或活動，未遵守我國法規。

(2)集中度風險

由於委外廠商的數量有限,提供的委外服務或產品僅集中在有限少數幾家。

(3)聲譽風險

委外廠商的業績不佳或形象不佳，亦導致公眾形成了對金融機構(委託機構)的負面形象。

(4)國家風險

金融機構資訊委外作業是外國服務提供商,該機構所位於之國家可能經濟、社會和政治條件皆處於不穩定狀態。

(5)作業風險

當委外廠商由於不當或失敗的內部控制程序、系統或外部事件和人為錯誤虧損，因而出現作業風險。

(6)法律風險

當委外廠商的服務提供出現異常，使金融機構面臨訴訟的法律風險。

(7)策略風險

委外廠商提供不正確的訊息，導致董事會及高級管理階層人員做出不合理的決策。

4.委外作業風險管理程序

資訊委外作業所衍生的風險管理程序相當重要，管理階層須嚴格監督，金融機構應謹慎分析及管理資訊委外作業所附隨的風險，包括瞭解相關作業的風險、透過謹慎程序遴選受託機構、績效評量及服務品質下降或停止營運時的緊急應變計畫，並建置對受託機構持續監督之計畫。

其風險管理原則如下：

(1)考慮是否進行資訊委外作業，董事會及管理階層應針對銀行整體的經營策略及目標，確認委外作業所要扮演的角色，方能完全整合至公司的策略目標

(2)委外作業前，金融機構必須確認其策略目標、效益、相關法規及成本，並包括作業委外相關風險，管理階層對委外作業應建立一套完整及實用的全盤式的評估確認程序。

(3)風險評估項目應包效益、內部控制 、服務水準的報告及契約是否符合法規，資訊人員、內部稽核人員、法規遵循人員與法務應一起分析委外作業的相關風險 ，建立必要的控制及報告架構 。

(4)金融機構必須有效確認受託機構是否有足夠資訊安全措施保護客戶資料與隱私。

(5)金融機構依策略計畫與風險評估項目，須建立評估資訊委外作業的標準，就委外作業終止，亦應建立適當的策略及緊急應變計畫。

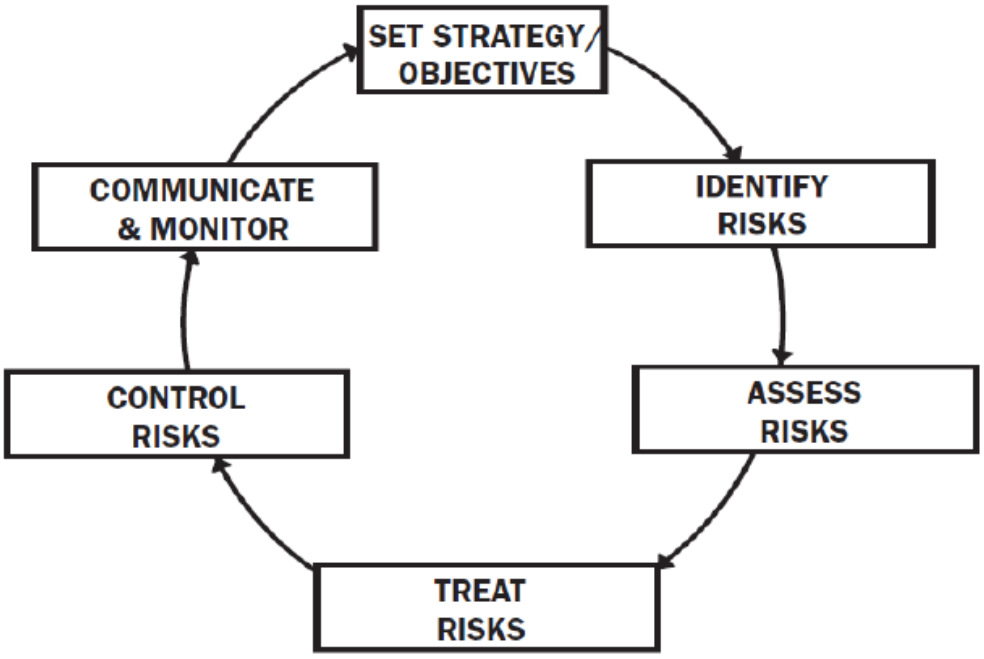
(6)管理階層應指派專人擔任監督資訊委外作業，從事評估與管理委外作

業及其與受託機構的關係 ，提供必要的資源以監督及衡量受託機構對委外作業的執行成效，並定期向董事會提出報告之責。

四、電子銀行/行動銀行科技風險管理

(一)科技風險管理策略目標

風險管理包括訂定因應風險的策略目標，然後識別、評估、降低或消除、控制、溝通及監控可能影響資訊系統的安全風險，決定風險管理是否符合策略目標之過程，使風險所造成的損失極小化。



Source: Adapted from Institute of Chartered Accountants in England and Wales, *No Surprises: The Case for Better Risk Reporting*, ICAEW, London, U.K., 1999, p. 47.

(二)科技風險評估方程式

資訊系統風險包含因意外或故意觸發資訊系統安全漏洞弱點(Vulnerability)的可能性所產生的威脅(Threat)，以及對組織產生的衝擊影響(Impact)程度，因此評估資訊風險可就弱點、威脅及衝擊三者相乘，而

計算風險值：

風險=漏洞 x 威脅 x 衝擊/概率

•弱點=一個系統錯誤設計所造成可操作的弱點

•威脅=一個惡意對手積極利用系統漏洞所能造成的危害值

•影響=漏洞會被利用而成為有害或威脅的可能性，

•概率=可能性衝擊。

(三) 科技風險實務管理要點

(1) 金融機構使用何種測試工具來檢測網站和行動應用程式。

(2) 金融機構是否頻繁更新網站和行動應用程式。

(3) 測試報告是否包括安全漏洞風險等級的分類和風險評估

(4) 在測試過程中所發現之安全漏洞，金融機構管理是否有效跟進修補應用系統

五、電子銀行/行動銀行檢查實務與國際監理經驗交流

(一)SR 參考指引(SR References)

美國監理機關所發布的電子銀行/行動銀行重要 SR 參考指引如下，通常亦為美國檢查實務重點項目：

(1)SR16-10: FFIEC Information Technology Examination Handbook – Retail Payment Systems Booklet（FFIEC 資訊科技業務檢查手冊-零售支付系統小冊子）

(2)SR 13-19: Managing Outsourcing Risks（管理委外風險）

(3)SR 11-09: Interagency Supplement to Authentication in an Internet Banking Environment(網路銀行環境之身分驗證補充說明)

(4)SR 06-13: Questions and Answers Related to Interagency Guidance on Authentication in an Internet Banking Environment（網路銀行環境之身分驗

證問答集）

(5)SR 05-19: Interagency Guidance on Authentication in an Internet Banking Environment（網路銀行環境之身分驗證監理指引）

(二)電子銀行/行動銀行檢查實務重點

電子銀行/行動銀行之檢查實務主要是以 FFIEC 資訊科技業務檢查手冊為參考基礎，**並配合監理機關所發布的 SR 參考指引及研討會課程內容，整理檢查實務重點如下：**

1. 電子銀行/行動銀行整體架構檢查實務重點

(1)了解底層技術的基礎設施架構，方能發現金融機構、委外廠商，甚至客戶之間的風險因子及如何控制或緩解風險，並找出誰有權執行控制或緩解風險。

(2)確認 IT 人員將資訊科技資源配置方式有效率地分配到電子銀行/行動銀行平台之電腦硬體、週邊設備、軟體及技術服務，圍繞著技術或組件所產生的風險，將會影響控制或緩解風險的決策。

(3)確認電子銀行/行動銀行平台處理資料須具備保密性（Confidentiality）、完整性（Integrity）及可用性（Availability）。

(4)設計階段是否依系統開發程序所規定之流程開發，開發階段是否做源碼檢測及修復建議,測試階段及上線維運階段是否有部署資安設備提供防禦功能，並監控及追蹤漏洞攻擊。

(5)定期執行弱點掃描及滲透測試並有稽核機制審查追蹤弱點漏洞修復狀況。

2.身分驗證機檢查實務重點

(1)由受信任的第三方驗證

(2)邏輯驗證來源之間的資料是否一致及查核客戶是否有詐欺行為記錄

(3)身份驗證應該產生稽核日誌，應定期監測和報告以檢測異常活動

(5)須使用多因素驗證機制之強身份驗證

(6)新開戶之客戶特別需要強身分驗證機制

3.密碼規則檢查實務重點

除了數位憑證和公鑰基礎設施（PKI），軟體代碼器(Soft Token)及硬體代碼器(Physical Token)等此類機制的安全檢核，身分認證的重點仍是密碼，實務做法如下：

(1)密碼複雜性:密碼長度、使用非字母(英數混合)、密碼歷程至少保存 3 代，不要使用詞典之單字。

(2)提醒客戶密碼到期和更新程序

(3)客戶帳戶登入多次失敗的嘗試則須予停用。

(4)只有使用者知道自己的密碼

(5)密碼透過網絡傳輸須以加密通訊

4.網路漏洞檢查實務要點

(1)攻擊在數量和複雜性繼續增加，基於這些新的和不斷變化的威脅，組織應更新其風險管理架構。

(2)高級管理階層和董事會應該了解並及時更新有關這些網路漏洞威脅的情報

(3)是否及時修補及更新所有系統安全漏洞，內部是否定期追蹤複掃以驗證是否落實系統漏洞修補？

4.帶自己的行動裝置來上班(BYOD)檢查實務要點

⑴從安全威脅和控制的角度，考慮 BYOD 對業務功能的影響和使用者管理解決方案的政策。

(2)找出什麼樣行動裝置管理(MDM)政策可以執行，政策是如何管理並實施測試和驗證，及其配套設施。

(3)是否要求員工註冊個人的手機，一旦該員工的手機遺失，資安人員是

否可透過控管平臺進行遠端刪除員工存放公司的資料 APP 及所有資料(遠端擦除行動裝置資料技術)。

5.源碼檢測及滲透測試檢查實務要點

(1)是否將敏感資料，如：憑證資訊、帳號、密碼等存放於開放式的儲存媒體(例如：SD 卡)，若敏感資料存放於開放式的儲存媒體，則須採用安全的加密措施並設定手機檔案的讀取與寫入權限等。

(2)檢查手機部分應用程式是否會儲存敏感性資訊，是否可加以手動移除，或是選擇不自動儲存功能。

(3)程式開發人員是否於伺服器端開發應用程式時以 OWASP Web Top 10 做為安全檢核參考。

(4)傳輸媒介包含網路連線、Wifi 連線，甚至是近距離通訊(Near Field Communication, NFC)連線等，若只採用明碼傳遞，攻擊者可輕易透過網路監聽方式(Sniffer)竊取機敏性資料，傳輸資料時，程式開發人員是否有確保所有敏感性資料有採用加密方式進行傳輸。

(5)網頁應用程式傳遞參數給後台系統，是否過濾不受信任或不應該接受的內容，如：SQL 執行語法及特殊字元等。

(6)是否使用嚴謹的身分驗證與授權，如：雙因素或多因素認證，避免只使用行動裝置的永不變的 ID 識別碼或身分顯性資料做為身分驗證的因素。

(7)應用程式在設計時是否注意身分認證與授權的問題，以確保行動裝置需經過使用者的身分驗證後才允許執行特殊的行為或功能。

(8)開發應用程式是否使用強度加密演算法，直到應用程式開發完成時皆不斷進行反覆測試。

(9)程式開發者是否避免將敏感資訊寫入於原始程式碼中。

6.資訊作業委外檢查實務要點

(1)資訊委外作業，金融機構董事會及管理階層是否確認其策略目標、效益、相關法規及成本，並包括作業委外相關風險。

(2)金融機構管理階層對資訊委外作業是否建立一套完整及實用的確認程序，做全盤式的自我評估。

(3)風險評估項目是否包括效益、內部控制 、服務水準的報告及契約是否符合法令規定條款。

(4)資訊人員、內部稽核人員 、 法規遵循人員與法務是一起分析委外作業的相關風險並建立必要的控制及報告架構 。

(5)受託機構是否能有足夠資訊安全措施保護客戶資料與隱私。

(6)是否建立評估資訊委外作業的標準，就委外作業終止時是否建立適當的策略及緊急應變計畫。

(7)管理階層是否指派專人擔任監督資訊委外作業評估與管理委外作業及其與受託機構的關係

(8)委外作業專責單位是否定期監督合約執行情形並向董事會提出報告。

7.個案研討群組分享之其他檢查實務要點

(1)電子銀行/行動銀行連線交易是否使用多因素驗證

(2)在一個持續的基礎評估新的身分驗證風險時，驗證機制是否進行適時更新。

(3)電子銀行/行動銀行相關網路各項資安設備是否已建立妥適的定期監控機制和日誌紀錄的備份及管理？

(4)針對金融機構對電子銀行/行動銀行系統資源存取授權情形，如：硬碟空間、記憶體及 CPU 負載等，是否建立監控機制並留存稽核軌跡供定期檢視。

(5)行動銀行是否注意行動裝置有越獄或 root 以取得最高權限？感染病毒？遺失位置？異常使用行為?

(6)是否開放 Wifi 存取以 BYOD 內部網路業務伺服器?

(7)檢查報告如果使用評級，查核結果是否為滿意、需要改進或不滿意?

(三)國際監理經驗交流

在座學員多為三年以下之資淺金融 IT 監理或檢查人員，除了詢問課堂一些關於 We b 伺服器弱點及應用程式測試等較細節的技術問題，不擬贅述，學員間有下列問題交流討論：

1.香港學員提問：請問行動銀行交易資料(手機 APP 存取的資料)到底要存在手機裝置上好，還是存在銀行端系統較好，我一直想要發相關的監理指引，但難以下決定：

Fed 講師群的回答：在美國，我們很重視聲譽風險，我不能明確跟你說那種方式較好，要看個別銀行的資安政策及系統架構是否安全，銀行是否已評估資料儲存位置的風險。

台灣(我國)學員檢查經驗分享：

(1)依台灣的檢查實務經驗，我們原則是建議受檢機構不要將敏感資料存放於手機裝置的儲存媒體 SD 卡，如：身分證字號、帳號及密碼等，甚至包含行動銀行與相簿連結的本人照片連結(Link)等，也須保護其存取權限。

(2)但若為方便客戶使用 APP，允許客戶可勾選記憶身分證字號及密碼而不用輸入，因而需將上開敏感資料存放於開放式的儲存媒體，則須採用安全的加密措施後方得儲存，且須提示客戶對手機檔案的讀取與寫入要設定權限。

(3)我個人的觀點及台灣銀行資訊系統實務經驗，行動銀行交易資料，如：身分證字號、帳號、存提金額、對方帳號及網路 IP 等以電文方式傳給行動銀行後台系統，並以日誌方式留存稽核軌跡，儲存後台系統是比較安全的作法，因為行動裝置可能丟失、遭 Jail Break 或 root 破解，銀行資訊系

統網路有較多的資安設備防護監控,應可比個人手機的防護層次較高也較為周全。

2.香港學員提問：請問行動銀行山寨版 APP（Cloned APP）而以釣魚方式(Phishing)誘騙客戶使用，雖然香港有要求銀行要隨時監測及通報釣魚網站及山寨版 APP，但目前有無可行之資安防護方法?

台灣學員(我國)檢查經驗分享：

依台灣的檢查實務經驗，我們正在考慮是否要推動行動銀行 APP 自主檢測機制，目前暫無強制，但會利用實地檢查，建議受檢機構要有適當檢測機制，包含 APP 是否被複製竄改(山寨版 APP)、最小權限審核取得原則、行動裝置是否遭遭 Jail Break 或 root 破解及是否執行源碼檢測及滲透測試、是否有 OWASP Top 10 的風險等，至於山寨版 APP 及釣魚網站，目前是由我國各銀行自主檢測在其網銀首頁公告，有時並沒有公告，而香港強制要求監測及通報而建立之統一通報機制可值借鏡，使民眾容易從單一網站了解並能安全的使用行動裝置。

Fed 講師群的回答：

在美國目前對行動銀行 APP 並無任何建議或強制措施，因為我們的監理文化重視多元獨立的監理制衡及聲譽風險，且受檢機構從大規模的金控銀行至極小規模的社區銀行差異很大，不會明確跟受檢機構說你必須做那些檢測較好，而由檢查人員視個別銀行的資安政策及系統架構評估後，要求受檢機構自行辨識評估行動銀行 APP 風險，並由受檢機構自行提出其緩解之道。

3.亞美尼亞學員提問：

雜湊函式法(Hash)是否就是代碼化(Tokenization)，兩者有無差別?

Fed 講師群的回答：

Tokenization 是指將卡號/帳號以一個某種隨機編碼的序號（稱為

token）來替代而進行交易，如信用卡持卡人要付款時，先透過手機連接「token 服務」，把卡號/帳號變成一個 token ，然後將 token 透過某種傳輸介面傳給商家,這 token 只能使用一次及在特定時間內對特定的手機與商家有效,所以任何人包括商家在內,在特定時間後即使取得 token 也沒有用，商家收到 token 後，再透過收單行傳給國際組織網路，再傳給發卡行，發卡行在透過相同服務還原這個 token 成為卡號/帳號，然後完成交易授權，授權成功之後，商家會得到一個針對該 token 的授權序號，商家憑此就可以進行後續的請款。由於交易過程代碼化無需信用卡相關資訊，可解決卡片資訊被盜用的問題。 Visa、Master、AE 與 Apple 一起實施上述的概念，**Apple Pay 就是 Tokenization 的行動支付系統例證。**

雜湊函式法 Hash 是一種演算法，將訊息或資料壓縮成摘要，建立一個雜湊值（hash values）的指紋，雜湊值通常用檢查資料的完整性，Tokenization 或許可用部份雜湊函式來完成，但目前雜湊函式主要是用於檢查資料的完整性(Integrity)，Hash 與 Tokenization 是不同的概念，不可混淆。

伍、 心得與建議

一、電子銀行/行動銀行系統之檢查建議以應用系統架構及配合軟體發展週期安全風險為查核主軸

1. 由本次研討會可知，美國是採由上而下(Top-Down)的查核方法，先評估各種層次的網頁(Web)、應用程式(AP)及資料庫(DB)伺服器在網路的部署位置與相關技術風險，再就上開伺服器之應用發展階段週期所對應相關的網路漏洞風險和攻擊，依階段查核所實施源碼檢測、弱點掃描及滲透測試並部署提供防禦功能之資安設備。

2. 美國以整體風險評估之查核角度值得借鏡，建議本局未來若辦理金融機構之電子銀行/行動銀行系統專案檢查，可採納美國由上而下的查核方法，以應用系統架構及配合軟體發展週期安全風險為查核主軸，評估電子銀行/行動銀行系統之整體風險。

二、推動行動銀行應用 APP 前後台資訊系統的自主安全檢測

本局今年(105)年初開始將行動(手機)銀行應用 APP 的資安問題列為檢查重點，這方面可算是少數獨步領先全球的國家，依本局實地檢查經驗，受檢單單位有將敏感資料(身分證字號、帳號及密碼)等存放於手機裝置的儲存媒體，也有取得民眾手機身分識別、聯絡人、檔案及簡訊等相關權限，進而建議受檢機構要有適當檢測機制，包含 APP 是否被複製竄改、最小權限審核取得原則、行動裝置是否遭 Jail Break 或 root 破解、是否執行源碼檢測及滲透測試等，美國講師及與會各國學員紛紛表示他們目前對 APP 尚未發布資安管理規範及資安檢測建議，我國對行動(手機)銀行應用 APP 的資安檢查經驗值得各國借鏡參考，因此持建議持續推動行動銀行應用 APP 前後台資訊系統的自主安全檢測。

三、持續關注帶自己的行動裝置來上班(Bring Your Own Device，BYOD)風潮，建議列為檢查重點

資訊作業之 BYOD 在美國風潮漸起，我國部分金融業者已著手打造雲端辦公系統，讓員工可使用自己的手機或平板電腦等行動裝置以 Wifi 無線存取內部業務系統，我國銀行業者亦有部分開放 BYOD 存取電子郵件及公文表單系統，面對金融業逐漸開放之 BYOD 風潮，建議本局將金融機構 BYOD 管理規範及落實程度，包括密碼保護、防毒防駭、硬碟加密、監控網路攻擊和客戶個人資料之存取及遠端擦除行動裝置資料技術等納入檢查重點。

四、建議參考成立資訊科技風險實驗室以提昇檢查人員專業深度及查

核能力

美國芝加哥聯邦準備銀行，為因應金融資訊科技創新及發展，成立資訊科技風險實驗室(STREAM Technology Lab)，建置軟硬體設備並配置專業 IT 檢查人員負責蒐集資訊安全技術最新資訊，在實驗室架設伺服器予檢測驗證，成果除了實際應用於檢查實務上，亦設計規劃課程提供美國聯邦體系及全球金融監理人員教育訓練，此次講師回答亞美尼亞學員所提問之雜湊函式法(Hash)及代碼化(Tokenization)之差異，此種對技術細微的深刻瞭解，即予各國學員深刻的印象，反觀我國無類似的教育訓練機構，建議未來可由國內金融教育訓練機構如金融研訓院，成立類似 STREAM 的金融資安實驗室，針對新興金融科技業務涉及電腦交易安全設計，評估潛在資安風險及妥適控管機制，以提昇本局及金融機構資訊業務檢查人員整體專業查核能力。

五、加強國際金融資訊科技監理交流，建立合作機制

本次研討會美國講師與韓國學員分別分享目前國際行動支付平台 Apple Pay 及 Samsung Pay，將信用卡資訊轉化為一組虛擬代碼(Tokenization)，用手機就可完成支付交易。可惜我國的廠商手機銷售量尚無法達到如美國 Apple 公司及韓國 Samsung 公司 之經濟規模，推出我國自己的支付平台，另由於我國金融業市場過小，要掌握全球支付市場平台發展契機並強化自己的金融科技學習經驗與實力，經由與上開國際行動支付平台合作以拓展跨境金融市場版圖是可行之道。

Apple Pay 及 Samsung Pay 以虛擬代碼化之金融科技之創新，顯示科技正在改變金融內涵，如何評估跨境、跨產業及虛實整合之遠距電子支付科技風險並建立準確有效之身分認證機制與詐欺偵測機制，美國、韓國及各國監理檢查機關也尚在摸索成長中，各國應可互相借鏡監理經驗，建構一套新興金融科技風險評估之

監理機制。

此外除了在課堂上與各國分享我國今年年初對行動銀行的實務檢查經驗，比較行動銀行交易資料及日誌稽核軌跡儲存前端手機與後台系統的安全差異，也利用午餐休息與各國學員閒聊 Swift 系統遭中間人攻擊（ Man in the Middle）攻擊方式之檢查經驗；而美國講師及學員閒聊美國幅員廣大，監理權力須互相制衡避免獨大，監理文化強調多元而獨立；香港學員則分享對 Cloned APP 及釣魚網站，強制要求銀行監測及通報而建立統一通報機制的金融消費者保護及宣導政策，都是互動良好的互惠交流經驗，本次受訓所結識之監理人員，所建立之良好情誼，可作為日後監理或檢查之諮詢來源。